Winter 2012 Software Assurance Working Group Sessions
Agenda (as of November 20, 2012)

MITRE-1, 7525 Colshire Drive, McLean, VA 22102

27 November (Tuesday) *8:30 AM – Registration*	28 November (Wednesday) *8:30 AM – Registration*		29 November (Thursday) *8:30 AM – Registration*
9:00 AM Opening	*9:00 AM Opening*		*9:00 AM Opening*
KSAs and Competency Model for SwA and SCRM (Auditorium)	***Track 1 - Workforce Education and Training Planning (1H300)***	***Track 2 - Technology and Tools and Processes and Practices (Auditorium)***	***Science and Technology Day (Auditorium)***
Software Assurance Professional Competency Model • Lauren Majdosz, Booz Allen Hamilton **SwA Competency Model** • Carol Woody, SEI **SwA and SCRM KSAs for the National Initiative for Cybersecurity Education (NICE)** • Dan Shoemaker, UDM	**Discussion: What should we be teaching?** • Dan Shoemaker, UDM	**Review and Interactive Discussion of DISA's Mobile Application Security Requirements Guide (SRG)** • BC Eydt, DISA **How do we handle Software Assurance with 3rd party modules?** • Josh Bressers, RedHat	**Innovation through funded research and community exchange** • Kevin Greene, DHS S&T **9:45 – 10:15 Break** **Homeland Open Security Technology (HOST)** • Luke Berndt, DHS S&T
10:30 – 11:00 Break	**10:30 – 11:00 Break**		**11:00 – 11:15 Break**
Interactive Discussion: SwA and SCRM KSAs and Competency Models	**WET Deliverables Planning** • Dan Shoemaker, UDM	**Process and Technology Out Brief From The NIST SCRM Workshop and Interactive Discussion on the NIST SCRM SP Outline** • Jon Boyens, NIST	**Collaborative environment to support continuous assurance services** • Kevin Greene, DHS S&T
12:30 – 1:30 Lunch	***12:30 – 1:30 Lunch***		***12:30 – 1:30 Lunch***
Organizational Initiatives for Supply Chain Risk Management (SCRM) • Elizabeth McDaniel, IDA **Out brief from the Global Forum on Digital Futures** • Dan Shoemaker, UDM **UK Trustworthy Software Framework (TSF)** • Ian Bryant, TSI	**Review and Interactive Discussion of the OMG Structured Assurance Case Metamodel Revision Task Force** • Bob Martin, MITRE **Updates To The "Key Practices For Mitigating The Most Egregious Exploitable Software Weaknesses" Pocket Guide** • Bob Martin, MITRE **Interactive Discussion of "An Assurance Tag for Software Binaries"** • Bob Martin, MITRE		**Key Terms in contracting for SwA and SCRM** • Joe Jarzombek, DHS • James Lindley, IRS
3:00 – 3:30 PM Break	***3:00 – 3:30 PM Break***		***2:30 – 3:00 PM Break***
SwA Executive Course Overview and *Interactive Discussion* • Carol Woody, SEI ***Interactive Discussion:* Education Initiatives**	**Third Party Assessments** Moderator: Joe Jarzombek, DHS Panel Members: • Fiona Pattinson, atsec • Ben Calloni, Lockheed Martin (Invited) • Bob Williams, SAIC • Paul Anderson, GrammaTech • Terence Rountree, GSA (Invited) • John Lindquist, EWA • Bob Torche, US Army • Bob Martin, MITRE		**NSF's Secure and Trustworthy Cyberspace (SaTC) program** • Leon Osterweil University of Massachusetts Amherst • Adam J. Lee, University of Pittsburgh • Heng Yin, Syracuse University • Gang Tan, Lehigh University • Dmitry V. Ponomarev, State University of New York • Jon Solworth, University of Illinois at Chicago • Xinyuan (Frank) Wang, PhD George Mason University • Tim Sherwood, University of California-San Diego • Nael Abu-Ghazaleh State University of New York at Binghamton • Clark Barrett, New York University
5:00 PM Wrap-Up	***5:00 PM Wrap-Up***		***5:00 PM Wrap-Up***

Tuesday - KSAs and Competency Model for SwA and SCRM (Auditorium)

Software Assurance Professional Competency Model - The Software Assurance Professional Competency Model is internal for DHS CS&C; yet it can serve as an exemplar for developing other SwA Professional Competency Models that have more limited scope in the functions of the professionals.

SwA Competency Model - The Software Assurance Curriculum team is developing a software assurance competency model. The model is based on the MSwA Knowledge areas, and will ultimately be mapped to the DHS Software Assurance positions, as well as to example government and industry positions in software assurance. This work is being developed in a manner that is consistent with the IEEE Computer Society Professional Activities Board competency framework. At this work session, we would like to get feedback from the WET WG on a partially completed version of the model.

SwA and SCRM KSAs for the National Initiative for Cybersecurity Education (NICE) - What are the true requirements that a software engineer, procurement officer, program manager, etc. needs to understand, do and audit with respect to software assurance and SCRM?

Organizational initiatives for Supply Chain Risk Management (SCRM) - The foundation of a comprehensive strategy for education, training, and awareness about global ICT supply chain security is the identification of the key organizations in the landscape. Using The Brain software, the team at IDA that is supporting the CNCI, NICE, and the Department of Defense is constructing a model to identify organizations and their key stakeholders. These key organizations and their training and educational components are prospective partners in spreading the word as appropriate to decision makers at every level; specialists who play important roles along a product life cycle; and leaders who make important policy, budget, and organizational decisions that relate to asset, system, and mission assurance. The Brain is also the repository for core messages, content, slides, and resources.

UK Trustworthy Software Framework (TSF) - This presentation summarizes recent activity on producing consensus guidance both by the Trustworthy Software Initiative (TSI), UK's equivalent to Software Assurance, and by related international standardization projects. TSI has recently1 published its Trustworthy Software Framework (TSF), which aims to provide an impartial means of understanding various domain specific terminologies, Citations, Methodologies and Data-sharing techniques (CMD). ISO/IEC JTC1 SC27 WG3 are in parallel working on a project entitled "Secure System Design Principles and Techniques"(ISO/IEC 29193), which aims to produce a publicly available specification of the subset of consensus approaches needed to realize trustable systems. Ian Bryant has a leading role for both activities.

SwA Executive Course Overview and Interactive Discussion - The Software Assurance Curriculum team is developing a software assurance course for executives, specifically government executives involved in acquisition and development of assured software. During this work session we would like to get feedback from the WET WG on a heavily annotated course outline to factor into our course development.

Wednesday Track 1 - Workforce Education and Training Planning (1H300)

Interactive Discussion: What should we be teaching? - What does it mean to understand and build expertise in trusted ICT as a field of study? What is an appropriate set of KSAs? What learning objectives map to the appropriate set of KSAs? What are WET Deliverables to support the answers: unified common body of knowledge, taxonomy, and definitions of SwA and SCRM.

Wednesday Track 2 - Technology and Tools and Processes and Practices (Auditorium)

Review and Interactive Discussion of DISA's Mobile Application Security Requirements Guide (SRG)

DISA Field Security Operations (FSO) is developing the Mobile Applications Security Requirements Guide that will define information assurance controls for mobile applications used in DoD. FSO has recently completed its review of community comments received on the public draft released 27 September 2012. This interactive session will include a discussion the content of the revised draft that will be presented to the Defense Security Accreditation Working Group on 11 December 2012. DISA Chief Information Assurance Executive signature is expected in January 2013.

How do we handle Software Assurance with 3rd party modules? - Today it is nearly impossible to build a product without using 3rd party software in some way. Maintaining 3rd party code in a product can be difficult. Who is responsible for updates? Who is looking for security issues? Did a vendor fix a security issue? Are there enough details about a security issue to decide if we're affected? This can be even further complicated when you bring open source into the mix. Open source is similar to shipping 3rd party modules, but with a few added twists. In this interactive session we will discuss the current challenges Red Hat faces in keeping code we did not write secure and how these "lessons learned" could be implemented in your organization through training and development practices.

Third Party Assessments Panel - What is a Third Party Assessment? How do software customers interpret assessment findings? Absent a consensus on assessment standards of practice and process, how can risk assessors provide acquirers a consistent insight into the assurance case for the software they are considering? Coding practices and development processes lack transparency and the third party assessors may not be giving customers much comfort if assessments cannot be compared. How can the SwA Community facilitate the maturation of this this growing industry by encouraging third party assessment methodologies that are robust, effective, comparable, and consistent? What is the relationship, if any, between process capability assessment and product assurance? Can we jump start this effort for software assurance by mining lessons learned in successful efforts such as the SEI's Capability Maturity Model Integration (CMMI) and its ties to the SCAMPI process?

Thursday

Innovation through funded research and community exchange - This panel focuses on areas of innovation in Software Assurance funded by DHS S&T Cyber Security Division through the Broad Agency Announcement. The discussion is broadly directed at the Software Assurance community to help facilitate an exchange with the performers in specific areas of Software Quality Assurance. The panelist will share expertise in their specific area of innovative research; discuss existing gaps in State of the Art tools and techniques, and discuss ways to improve the overall quality of software through improved testing and evaluation capabilities.

Homeland Open Security Technology (HOST) - The Homeland Open Security Technology (HOST) program is DHS S&T's project to look at helping federal, state, and local government use Open Source cybersecurity solutions gain new capabilities and improve efficiency. While open source software should be considered as an option in many instances, there are challenges for government in successfully finding, acquiring, maintaining and operating open source software. Generally policy allows for it, however cultural and procedural changes may be required. This session will explain what the HOST program is doing to help address these issues, what existing efforts have been leveraged, and provide initial research findings.

Collaborative environment to support continuous assurance services - By offering the capacity needed to continuously analyze and test a rich and evolving collection of open-source software packages and customized applications, the Software Assurance Marketplace (SWAMP) will help the software assurance community improve the quality and reliability of software used to power our nation's critical infrastructure. This panel will discuss the collaboration needed between the community and performers to ensure the SWAMP is a success -- where software developers, software assurance tool developers and software researchers can meet to exchange ideas to improve overall quality of software, produce better performing tools, and discover new techniques for vulnerability discovery.

Key terms in contracting for SwA and SCRM – Contract terms require careful definition. For example, failure to agree on the meaning of "malware" or "tainted products" can lead to contract conflicts and misunderstandings, even substantial unanticipated risk exposure. What Software Assurance and Supply Chain Risk Management (SCRM) terms have been found to be problematic and why? What terms have caused miscommunication and confusion, are poorly defined, or aren't even defined in any source. What definitions have worked and what have not? Do the members of the SwA Community have recommendations for reasonably good definitions or authoritative sources of definitions?

NSF's Secure and Trustworthy Cyberspace (SaTC) program - NSF's Secure and Trustworthy Cyberspace (SaTC) program is one of the largest research programs at NSF, and one of the largest cybersecurity grant programs in the country. With over $70M/year in grants planned for FY13, SaTC covers a broad range of technical topics, as well as interdisciplinary connections in social and behavioral sciences, cybereconomics, cybersecurity education, and transition to practice. We have invited the principal investigators for over $32 million in Software Assurance (SwA) and Supply Chain Risk Management (SCRM)-related grants. Participants in the SaTC program will discuss with the SwA Community the issues being covered by these grants and whether there are gaps that shoud be addressed in current and future solicitations for proposals. We will also discuss the uptake of research findings and their impact on SwA process and practices, technology and tools, workforce education and training, measurement and business case, and malware and cyber observables. This discussion is most relevant with submission deadlines for medium proposals of Nov 30, small and cybersecurity education of Dec 14, and Frontier proposals of January 30 2013.

Save these dates!

- Summer 2012 Software Assurance Working Group Sessions
  25-27 June 2013, at MITRE-1, 7525 Colshire Drive, McLean, VA 22102-7539

- Spring 2013 Software Assurance Forum
  5-7 March, 2013 at NIST, 100 Bureau Drive, Gaithersburg, MD 20899